Centre for International
Governance Innovation

CIGI Papers No. 206 — December 2018

Four Internets
The Geopolitics of Digital Governance

Kieron O'Hara and Wendy Hall

Centre for International
Governance Innovation

CIGI Papers No. 206 — December 2018

Four Internets
The Geopolitics of Digital Governance

Kieron O'Hara and Wendy Hall

CIGI Masthead

Executive

President Rohinton P. Medhora
Deputy Director, International Intellectual Property Law and Innovation Bassem Awad
Chief Financial Officer and Director of Operations Shelley Boettger
Director of the Global Economy Program Robert Fay
Director of the International Law Research Program Oonagh Fitzgerald
Director of the Global Security & Politics Program Fen Osler Hampson
Director of Human Resources Laura Kacur
Deputy Director, International Environmental Law Silvia Maciunas
Deputy Director, International Economic Law Hugo Perezcano Díaz
Director, Evaluation and Partnerships Erica Shaw
Managing Director and General Counsel Aaron Shull
Director of Communications and Digital Media Spencer Tripp

Publications

Publisher Carol Bonnett
Senior Publications Editor Jennifer Goyder
Senior Publications Editor Nicole Langlois
Publications Editor Susan Bubak
Publications Editor Patricia Holmes
Publications Editor Lynn Schellenberg
Graphic Designer Melodie Wakefield

For publications enquiries, please contact publications@cigionline.org.

Communications

For media enquiries, please contact communications@cigionline.org.

@cigionline

Printed in Canada on paper containing 100% post-consumer fibre and certified by the Forest Stewardship Council® and the Sustainable Forestry Initiative.

Centre for International Governance Innovation and CIGI are registered trademarks.

Centre for International Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Authors

Kieron O'Hara is an associate professor in electronics and computer science at the University of Southampton, UK. His interests are in the philosophy and politics of digital modernity, particularly the World Wide Web; key themes are trust, privacy and ethics. He is the author of several books on technology and politics, the latest of which, *The Theory and Practice of Social Machines* (Springer, with Nigel Shadbolt, David De Roure and Wendy Hall), will appear in 2019. He has also written extensively on political philosophy and British politics. He is one of the leads on the UK Anonymisation Network, which disseminates best practices in data anonymization.

Dame Wendy Hall, DBE, FRS, FREng, is Regius Professor of Computer Science at the University of Southampton, UK, and an executive director of the Web Science Institute at Southampton. Her influence as one of the first to undertake serious research in multimedia and hypermedia has been significant in many areas, including digital libraries, the development of the Semantic Web and the emerging discipline of Web Science. She became a Dame Commander of the British Empire in 2009 and is a fellow of the Royal Society. She has been president of the Association for Computing Machinery, senior vice president of the Royal Academy of Engineering, and a member of the UK Prime Minister's Council for Science and Technology. She was a founding member of the European Research Council and chair of the European Commission's Information Society Technologies Advisory Group; a member of the Global Commission on Internet Governance; and a member of the World Economic Forum's Global Futures Council on the Digital Economy. Dame Wendy was co-chair of the UK government's review of artificial intelligence (AI), Growing the Artificial Intelligence Industry in the UK (2017), and became the UK government's first "Skills Champion for AI in the UK" in 2018.

About the Global Security & Politics Program

The Global Security & Politics Program at CIGI focuses on a range of issues in global security, conflict management and international governance — a landscape that continues to change dramatically. Such changes are widely evident in the growing rivalry between China and the United States in the Asia-Pacific and the emergence of new economic powers in the region, such as Indonesia; the divergent ways Canada, Russia and the United States perceive Arctic security as melting ice opens up the Northwest Passage; continuing debates about the humanitarian imperative as the world confronts new crises in Africa and the Middle East; and new areas of concern such as cyber warfare and the security of the internet.

With experts from academia, national agencies, international institutions and the private sector, the Global Security & Politics Program supports research in the following areas: Arctic governance; Asia and the Pacific; fixing climate governance; governance of conflict management, with a focus on Africa; global politics and foreign policy; and internet governance.

Acronyms and Abbreviations

AI	artificial intelligence
CNIL	Commission Nationale de l'Informatique et des Libertés
DNS	domain name system
FCC	Federal Communications Commission
GDPR	General Data Protection Regulation
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	IP version 4
IPv6	IP version 6
ISPs	internet service providers
SNSs	social networking sites
VoIP	Voice over Internet Protocol
W3C	World Wide Web Consortium

Executive Summary

The internet is not a monolithic architecture whose existence and form are guaranteed in perpetuity, but a fragile and contingent construction of hardware, software, standards and databases, governed by a wide range of private and public actors whose behaviour is constrained only by voluntary protocols. It is therefore subject to evolution and political pressure. Its original creators engineered it to be open, that is, that its standards should be transparent, and that data and software should be portable, extensible and interoperable. This Silicon Valley view was partly ideological, but partly based on engineering principles to enable the internet to scale as it grew. However, as the internet, and applications such as the Web, have become entrenched in daily life, competing views about how it should be governed have begun to emerge, and to be championed at the national level, where they are playing a geopolitical role. European nations, and the European Commission, envisage a "bourgeois" internet, where trolling and bad behaviour are minimized and privacy protected, possibly at the cost of innovation. Many nations, perhaps most notably China, see an authoritarian internet, where technologies of surveillance and identification help ensure social cohesion and security by combatting crime, terrorism, extremism and deviance. A more commercial view, characteristic of the US Republicans in Washington, DC, understands online resources as private property, whose owners can monetize them, exclude others from using them and seek market rates for their use. Finally, the openness of the internet is a vulnerability that can be exploited for misinformation or hacking, an opportunity taken by Russia, Iran and North Korea, among others. Thus, several internets are currently co-existing uneasily. We have not, however, reached an equilibrium; we need to be prepared for the internet that we know to evolve unpredictably, and work to ensure that it remains beneficial for humankind.

Introduction

The internet is not a monolithic technological creation, but a congeries of systems, protocols, standards, hardware (the infamous "tubes"; Blum 2012) and organizations. It encompasses the domain name system (DNS), information intermediaries, security systems, exchange points, autonomous systems, internet service providers (ISPs), registers, databases and standards bodies — some with national standing, some (often in the United States) with global reach, and others of international standing — as well as some public bodies, some private companies and some non-profit organizations.[1] The system is truly socio-technical — we cannot hive off the technical from the rest. Every design decision reflects, and imposes (perhaps unconsciously), a balance of power, while cultural, economic and political tensions play out across the collective-action problems generated by digital modernity (O'Hara 2018). Neither computer science nor the social sciences are individually sufficient to understand this immensely complex piece of technology, the structure of which is driven by the people who upload content, download content and create the links; the authors of this paper have long argued that a dedicated "Web Science" is required both to understand it and to engineer it (Berners-Lee et al. 2006; O'Hara et al. 2013; O'Hara and Hall 2013).

To complicate the politics, the internet grew out of several US initiatives, and the United States retains a disproportionate influence. However, this position, which has fostered the growth of the internet for decades, is under pressure. International bodies have called for responsibility for the internet to be transferred to more international arenas — for example, the Working Group on Internet Governance, under the auspices of the International Telecommunication Union, recommended in a 2005 report (paras. 52, 55) that the United States relinquish oversight of the system, the role ideally to be performed by a UN body. The aim of such measures is to replace the current ad hoc, decentralized, distributed model of internet governance with a system of greater legitimacy; the danger, however, is that such a system would become centralized and sclerotic,

1 As described by Laura DeNardis (2014a), to whom this paper's authors are indebted for many insights.

focused on government power rather than on the inclusion of, say, civil society or industry voices. Arguments between democratic and non-democratic states, for example, are likely to dominate such a forum, with the risk of reducing it to stalemate. Accordingly, such proposals have struggled to find support, in part because few doubt that the United States has, on the whole, been a benign force on the internet and nurtured its growth as few other nations could or would. As a result, many commentators, by no means all American, believe that the United States' hands would be far safer than the United Nations'.

More important than this diplomatic pressure to change the system, therefore, has been the application of power by various national and supranational institutions to the delicately balanced system itself, to try to "push" the internet into a different type of model. This *realpolitik* is having an effect, and it is clear that the internet, as originally conceived by the primarily American white male technologists who founded it, is morphing into something else. But what?

The internet has many possible futures: it could break or collapse under these pressures, as was recently argued by Eric Schmidt, former chairman of Google and Alphabet (Kolodny 2018); it could develop unequally, with few if any benefits for the half of humanity that is not connected; or it could flourish over a diverse set of technologies and geographical areas (Global Commission on Internet Governance 2016). Progress at the moment is equivocal. In this paper, the authors will argue that four internets — at least — are emerging. They are, at present, coexisting, and may continue in this way for some time. It is possible, however, that any of these internets may fall by the wayside, and also that any one of them might become dominant — or, indeed, that the whole intricate system may collapse from these pressures.

The Creation and Governance of the Internet

In the context of clashing geopolitics, the internet is a gossamer arrangement. Its core is the naming system that gives one's device a presence, an identity, even a technical persona, on the internet itself. Identifiers have to be globally unique and universally accepted for the internet to function as a global space. The main identifier is the numerical Internet Protocol (IP) address (32 bits in length in IP version 4 [IPv4], 128 bits in IPv6), which is convertible by one of a number of recognized organizations into the familiar domain name. The link between IP addresses and domain names is maintained by a hierarchically federated database.

The DNS is extraordinarily complex, with several tasks to be coordinated in real time and at scale in order that the essential system of unique naming be preserved. Domain names need to be assigned, and to be resolvable into IP addresses via the database; the database needs to be edited and maintained; the hierarchical naming structure needs to be edited and maintained (for example, authorizing new top-level domains on a par with .com or .org); the servers containing this material need to be operated and housed; new language scripts beyond the Latin alphabet need to be authorized and integrated; disputes need to be resolved in a timely and legitimate fashion; and, not least, the system needs to be secured from attack.

There are many other aspects to internet governance, all equally complex, and requiring intricate engineering and institutional coordination across governmental and private bodies, and across borders. The internet has a particular history, rooted in Silicon Valley, and has been extraordinarily successful. However, this history is contingent; it could have been designed differently and it could change over time. This paper will consider some of the forces for change that are already altering a structure that is sometimes taken for granted.

Openness

Internet governance bodies are reflexively open. The Internet Engineering Task Force (IETF), which develops open internet standards, is highly participatory and transparent. Participation is not restricted by credentials, and the IETF's documentation and records are open and freely available, allowing oversight and accountability. The IETF prefers to approve standards that do not rest on intellectual property and patents; where these do exist, it prefers royalty-free licensing. The World Wide Web Consortium, or W3C, has a similar policy with open standards and opposition to royalties, although it has a membership model and accepts institutions of any kind as members.

Openness of governance begets openness of technology. Until relatively recently, the operation of the network ignored the content of the packets of information that were routed around it. Routing algorithms applied to all packets indiscriminately, and the routers had no access to the content to derive grounds for discrimination. The headers of the packets, which contain the metadata about, for example, where the packets are headed, were the only things read. In this sense, there was no interference with the flow of information around the internet.

Support for this open system is often very idealistic. Yochai Benkler argues in his book *The Wealth of Networks* (2006, 131) that "the emergence of less capital-dependent forms of productive social organization [offers] the possibility that the emergence of the networked information economy will open up opportunities for improvement in economic justice, on scales both global and local."

Hence, admiration of the technical brilliance of the internet design combines with an idealistic view of its affordances (what it, as an environment, offers the individual), a view which itself bifurcates. The admirer of the technology approves not only of the speed and efficiency with which data can travel from A to B, but also more generally of free speech, free association and other aspects of individual liberty. The result is a libertarian vision of the internet focused on its affordances, somewhat divorced from any messiness resulting from its collision with quotidian offline existence. On this view, the brilliant and elegant design complements the excitement of the freedom it offers, and each becomes normative — the internet should be free, because its design frees people to develop authentically and autonomously.

The most famous statement of this philosophy is John Perry Barlow's "Declaration of the Independence of Cyberspace," which rejects any idea that cyberspace needs real-world institutions and remedies, arguing:

> Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.
>
> We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.
>
> We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.
>
> Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.
>
> ...The only law that all our constituent cultures would generally recognize is the Golden Rule. (Barlow 1996)

Concerns about Openness

Until recently, it was assumed that this philosophy of openness and liberty would carry all before it, but many of the challenges facing authoritarian opponents of openness 10 years ago (O'Hara 2009) have been overcome. Benkler's warm approval is not the only possible reflection on the design of the internet, especially when we think of that design as a socio-technical construct rather than as a set of elegant technical protocols. Most obviously, the very idea of openness — in trade, migration, capital movements and so on — is under threat across the globe following the 2008 financial crisis, and of course the open internet has been a key part of globalization. Furthermore, openness does not always guarantee equitable outcomes — Silicon Valley has been called "a monoculture of white male nerds" in which companies founded

by women received two percent of venture capital funding in 2017 (*The Economist* 2018s).

In particular, central to the internet's function is that the key resources, notably the devices by which the internet is accessed, are universal and unique. A website needs the contacting device's IP address in order to deliver the requested information to it (an IP address is regarded as identifying in at least some circumstances by the Court of Justice of the European Union[2]). Other unique identifiers are also vital for the internet's function, including various hardware identifiers, cookies, real-name requirements in social media, location information from IP addresses and mobile base stations, and the identification requirements associated with ISPs. The uniqueness upon which the system depends tends to spark three different responses.

The first is a *worry about privacy.* The function of the democratic world depends on reasonable privacy for individuals to consume news, political speech or other cultural artefacts; to associate without surveillance; and to organize action. The structure of the internet holds out the possibility that people, or at least their devices, can be traced, and their downloads and uploads noted and recorded. Attempts to solve this problem by using open standards to allow users to express their privacy preferences, such as the Platform for Privacy Preferences[3] and "Do Not Track" mechanisms,[4] have not caught on nearly as well as blunter instruments such as encryption standards, behind which both the innocent and the guilty can shelter.

The second response, the converse to the first, is to *welcome an opportunity*. Security and law enforcement loom large in the responsibilities of government, and the use of the internet as a communication medium gives the prospect of understanding criminal and terrorist networks that threaten public security. Furthermore, the patterns of interaction might also help to optimize certain social functions, allowing government intervention to use the data generated to improve matters. The increasing prevalence of mobile devices and the Internet of Things will extend the reach of such benign (or not so benign) governance, facilitating interventions in, say, health care and well-being, climate change and traffic congestion.

A third response to the internet's uniqueness is not perhaps quite as obvious as privacy concerns or the embrace of opportunity, but follows from reflection about the business models that the internet has ushered in. The identity infrastructure that underpins the internet is also the foundation of the *targeted advertising model* that finances online services ranging from search to social media to email to news to user-provided content. This business model has driven extraordinary innovation online, and created high-value network effects in accordance with Metcalfe's Law that the value of a network is proportional to the square of the number of nodes. Privacy may be a good that most people are willing to trade away, and so, on this argument, why should they be prevented from so doing?

Furthermore, in the current context where far more information is being created and shared, there may be reasons to revisit some of the assumptions underlying the internet's design. For instance, the early text-based applications in the internet did not really cause much of a problem when packets were indiscriminately sent hither and thither. However, when the internet is used for synchronous communication or other time-sensitive applications, there are limits to acceptable levels of latency, and certain media, such as video, consume scarce bandwidth. Using the market to solve issues of latency and bandwidth implies the development of property rights to allow infrastructure owners to make managerial decisions to hold up or speed up traffic, legitimizing the use of intrusive technologies such as deep package inspection.

This paper argues that each of these three responses to the internet's design, architecture and governance underpins a particular view of how it should be run, competing with the original purist libertarian vision. Hence, there are (at least) four possible internets. Moreover, each of these four visions has a powerful set of institutional and ideological champions, and they can all coexist — hopefully, but not necessarily, peacefully.

A coda: the internet requires design, standards and cooperative behaviour. This necessity implies one final response to the internet, a human response that elaborate systems tend to

2 *Patrick Breyer v Bundesrepublik Deutschland,* [2016] EUECJ C-582/14.

3 Described at www.w3.org/P3P/ and now obsolete. It demanded rather a lot of investment from users for only equivocal gains.

4 See www.w3.org/TR/tracking-dnt/; at the time of writing, this is a W3C recommendation, but it remains unclear what exactly it means when a user asks an application not to track her.

invite — *subversion*. Plain vandalism is a possible response to the complexity and elegance of the internet, and it appears in the form of deliberate and malicious information pollution — trolling being perhaps the most obvious manifestation. However, subversion has an aesthetic of its own, a hacking aesthetic that is pleased to undermine the basic functions or promises of a system, often by using those basic functions against the system itself. Accordingly, ideas such as fake news or the spreading of malware — interventions that would not be possible without the very infrastructure they are there to undermine — are important parts of the subversive's arsenal. The subversive aesthetic also drives a global position on the internet, originally a dispersed and ad hoc response that manifested itself as cybercrime and hacking, but which in more recent years has itself attracted institutional backers at the level of the nation state.

The Geopolitics of Internet Ideals

The ideals sketched above are not the only responses to the Silicon Valley ideology of openness, but they are important in 2019 as they all have institutional backing at the level of the nation state or supranational entity. Much of the internet revolves around standards, and an accountable, open and transparent standard-setting process. However, this does not mean that governments are not under pressure to intervene, as either regulators or developers, or via procurement (DeNardis 2014a, 84). Many nations, at least when going through idealistic and optimistic periods (often coinciding with economic growth), have supported open standards, as, for example, India and Brazil in recent years. However, many social effects of the internet, including the spread of social media, the perceived threats to individuals' (in particular, children's) psychological well-being, cybercrime, cyberwarfare and a coarsening of public debate, have led some governments to step in more assertively. Above all, the perception that the internet is of necessity a disseminator of liberal and democratic ideals has caused pushback (Morozov 2011). Certain issues, such as net neutrality (see below), or the extent of liability of content platforms or information intermediaries for the information they carry, fall directly within governments' remit to legislate or not.

Governments, therefore, do have power to shape the internet and to reconfigure the trust relationships on it, perhaps through what DeNardis calls the "dark arts" of internet governance (2014a, 199–221). For example, trusting the websites we access depends on the maintenance by Web browsers of lists of trusted certifying and authenticating authorities. However, such lists do not solve the problem of online trust, but rather shift it toward the authorities, which provide economies of scale in evaluating the trustworthiness of websites, but which also create the greater systemic risk of a global rather than a local model of trust (O'Hara 2004). Such a system is only as secure as the least common denominator. A government could compel a browser-trusted authority to certify an imposter mail server, for instance, to support surveillance of its citizens or residents in its territory (DeNardis 2014a, 95). In 2008, the Pakistani government took down YouTube in Pakistan using the tactic of requesting Pakistan Telecom to redirect YouTube's IP addresses (Hunter 2008). Routing systems were set up for a smaller and more socially homogeneous internet, where trust, good faith and similar aims could be assumed. Of course, the internet community responds to trust deficits with improvements in security technology, but any technical solution lives in some social, political and economic context as part of a socio-technical system that is much harder to predict or control than its technological component.

There are certain types of content that most governments try to curb, such as child pornography or pirated intellectual property. There are other areas, such as political discussion, Holocaust denial or blasphemy, where (a) only some governments wish to intervene, and (b) typically they do not agree on what to censor. However, this does not mean that they will not try. An important means for governments to control or censor the content distributed on the internet is to intervene in the protocols, the systems or the technology, as with the Pakistani takedown of YouTube. Such censorship is not unavoidable — the "dark Web" often provides technologies to circumvent such interventions — but it is pretty effective in stopping messages being disseminated through audiences whose interest is more casual.

These powers, however limited, mean that governments' actions are implementing different conceptions of what the internet can be. This section reviews the four internets of most prominence. In addition, this section considers another vision, not of the internet per se but of an important rogue model for understanding the trajectory of internet governance in 2019 and beyond.

Silicon Valley's Open Internet

Silicon Valley's open internet is mainly driven by the technology. Problems are expected to have technical solutions primarily, even if there may be issues about how to implement these. For instance, WhatsApp is making strides in slowing down the viral spread of fake news and dangerous rumours with technical means (which may be easier because it does not rely on an advertising model; see *The Economist* 2018l). With respect to privacy, the most prevalent view is to see a privacy breach as a tort (Prosser 1960), requiring the victim to show evidence of harm.[5] This common law approach to privacy fits in nicely with the Silicon Valley credo of "move fast and break things" — innovate until the innovation is shown to be harmful.

However, not all regulation is bad, on this view; regulation may be needed to ensure the unfettered flow of information. Net neutrality is a signature policy of the Silicon Valley open internet. It is the principle that internet providers should not discriminate between different types of packets of information transmitted over the internet, to give preferential treatment to some types over others. Discrimination might happen for engineering reasons (certain information-heavy and time-sensitive uses, such as video or game streaming, might clog up the network), economic reasons (a mobile operator might not wish to provide the infrastructure for free Voice over Internet Protocol [VoIP] services), or ideological reasons (an operator might wish to discriminate against child pornography, say, or the messaging of an opposition political party).

Net neutrality has more of an impact on the last mile of internet delivery than on global governance. In countries with sufficient competition between providers, it is less of an issue, because anyone who objected to such discrimination could simply switch to a provider that respected net neutrality. As an issue, it looms largest in the United States, where competition is relatively thin, and where free speech is a highly prominent shared and constitutionally enshrined value.

Engineers, including Vinton Cerf and Tim Berners-Lee, have tended to favour net neutrality because of its positive effects on the network's efficiency. Other supporters, however, have been motivated by business reasons; Google, Amazon and eBay want as much access to their popular sites as possible, while companies that offer VoIP services (such as Microsoft, which owns Skype), and streaming companies such as Netflix need to avoid their content being throttled or slowed down.

Brussels' Bourgeois Internet

Europe's political attitudes differ from those of the United States, whose political and public space are defined by a liberal creed. In Europe, history plays a much larger role — nation states have learned, through war, to focus on peace, prosperity and cohesion. The European Union was originally posited as an end point to these integrative processes, and, in cyberspace, it has taken it upon itself to defend a civilized bourgeois public space against incivility, taking action, for example, against disruptors such as Airbnb, which is blamed for swamping beautiful cities with tourists (*The Economist* 2018k). The European Union's Competition Commissioner Margrethe Vestager has extended the Commission's anti-trust work against dominant firms, based on article 102 of the EU treaty,[6] to pursue American tech giants on the ground that they might swallow rivals or force them out of business, leaving consumers with a poorer standard of service (*The Economist* 2017b).

The bourgeois world rests upon virtuous behaviour, civility and prudence (McCloskey 2006), and Western European governments by and large attempt together with the European Union to secure this world. Only in such an atmosphere of trust in government would it be likely that, for example, Swedes would take to inserting

5 Daniel Solove has written a series of blogs developing a theory about this. He argues that US courts tend only to see privacy breaches as harmful if they cause either physical or financial injury, and if the harm has already happened (ignoring risk of future harm) (Solove 2014).

6 *Consolidated Version of the Treaty on the Functioning of the European Union*, 13 December 2007, [2012] OJ, C 326/47, art 102 (entered into force 26 October 2012), online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN>.

microchips in their bodies so enthusiastically (*The Economist* 2018n). European thinking on ethics and privacy focuses on dignity, whereas the American tradition looks toward liberty (Whitman 2004), so it is not surprising to find an EU Ethics Advisory Group worrying about the relationship between personhood and personal data, the risks of discrimination as a result of data processing, and the risks of undermining the foundations of democracy (EDPS Ethics Advisory Group 2018).

European courts are regulating the internet increasingly aggressively. To take one prominent example, the Court of Justice of the European Union ruled against Google Spain in 2014 in a case brought by a man who wanted outdated information about him removed from Google's search results.[7] The original decision was a compromise, and a controversial one, although welcomed by many commentators, including the present authors (O'Hara 2015; O'Hara and Shadbolt 2015; O'Hara, Shadbolt and Hall 2016), as allowing the European Union to police its own jurisdiction without imposing its own restrictive view of privacy upon the world. However, since the judgment, the French data protection regulator CNIL (Commission Nationale de l'Informatique et des Libertés) has tried to push back against searches for EU citizens in any jurisdiction, and the General Data Protection Regulation (GDPR) of 2018 has enshrined that universalism into EU law, even switching the emphasis from delisting to erasure (Politou, Alepis and Patsakis 2018).

Many suspect it will be harder to innovate in Brussels' bourgeois internet, thanks to a preference for incumbents and distaste for disruptive newcomers. For example, the GDPR is perceived as a threat to the model of free services for surveillance (*The Economist* 2018c). The GDPR is a paradigm case of the European Union's drive to a bourgeois level of safety. In contrast to American law, it covers every kind of data processing, whether shown to be harmful or not, and tries to anticipate and minimize risk (although it has been argued that the box-ticking mentality it has promoted is in practice no more protective of privacy than the tort-based approach of the United States; see Bamberger and Mulligan [2015]). Yet, the GDPR remains a source of advantage for the European Union — it is a leader in data protection because it is too large a market to ignore. It is also totemic: "This new data protection ecosystem stems from the strong roots of another kind of ecosystem: the European project itself, that of unifying the values drawn from a shared historical experience with a process of industrial, political, economic and social integration of States, in order to sustain peace, collaboration, social welfare and economic development" (EDPS Ethics Advisory Group 2018, 6). The jury is out; the GDPR has certainly been influential worldwide. However, it may handicap Europe in the development of artificial intelligence (AI). Where China and the United States are each large centralized markets, enabling the gathering of giant quantities of data to fuel their algorithms, Europe is more fragmented, both in terms of markets and in terms of the dominant tech companies, and this decentralization is exacerbated by the GDPR's stern regulation of data sharing (China's data advantage is discussed in the next section).

Privacy is not, of course, the only area where the European Union's instinct is skeptical of market forces, which are sometimes perceived as too disruptive, creating social costs, and sometimes perceived as producing an incoherent or inefficient internet where private gain crowds out public gain. A satisfactory set of arrangements is simply inconceivable without a regulator. For instance, the European Union's update of its copyright laws[8] has attracted opprobrium because of its aggressive stance on copyright breaches (*The Economist* 2018u). Characteristic of the European Union's attitude toward technology firms is its assumption that complaints about regulation threatening the freewheeling, entrepreneurial internet are exaggerated. Article 13 of the new copyright law compels internet firms to work closely with copyright holders to bring down copyright materials as soon as possible, which (given the imprecise nature of copyright identification algorithms) is likely to result in overzealous policing. Article 11 requires aggregators to obtain a licence from publishers if they display excerpts from content. A similar rule introduced in Spain in 2014 led Google to withdraw its aggregation service from there; the bet underlying article 11 is that Google could not afford to do the same

7 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (13 May 2014), Doc C-131/12, ECLI:EU:C:2014:317 (CJEU).

8 The Directive of the European Parliament and of the Council on copyright in the Digital Single Market, at www.consilium.europa.eu/media/35373/st09134-en18.pdf.

across the whole of Europe. The European mindset is that reasonable behaviour is unlikely (if not impossible) in the absence of rules: one study for the European Union about the interconnection of the internet's autonomous systems concluded: "A recurrent theme in the discussion of IP interconnection is whether network operators will be motivated to interconnect (on reasonable terms) in the absence of a regulatory obligation" (quoted in DeNardis 2014a, 130). Meanwhile, some agencies are simply acting to try to influence, as, for example, the United Kingdom's Government Communications Headquarters helping UK cyber security firms (*The Economist* 2018o).

Government, on this model, is the primary locus of trust. It is doubtful whether this proposition would be supported (or supportable) on any of the other internets described in this paper.

Beijing's Authoritarian Internet

China's importance not only to the world economy, but also to the internet, has grown remarkably in recent years, so that over half the country is connected to the internet, and over half of internet users are in China. Even if one is skeptical of Robert Kaplan's claim (2018) that the classic geography of the Eurasian empires has returned, the new assertiveness of China has coincided with a shift in European and Asian geopolitics, which has led to a diminution of the constraints of behaviour on China (and also on Russia).

The internet, for China, has been a boon for surveillance. Technology, for example, is used to monitor restive populations such as that of Xinjiang province (*The Economist* 2018d). Protections against surveillance are being eroded across the globe, as the technology becomes easier to apply and people are more willing to behave in ways that make them easy to watch, such as social networking. However, the trend is particularly strong in China.

The Chinese model is based on the promotion of its own tech giants, Baidu, Tencent and Alibaba. These are private companies, astonishingly successful in their own right, but operating within a tightly controlled environment in which the ruling Communist Party is the dominant player. However, China also has an increasing presence on international bodies; for instance, it currently holds the chair of the International Telecommunication Union, which is pushing for standards that will aid government micromanagement of the internet.

China itself has begun to invest heavily in technology using venture capital models (*The Economist* 2018j). Alibaba and Tencent are among the largest of China's venture capital investors and are shaping the start-up world in that nation (*The Economist* 2018p). Beyond that, Chinese companies have invested billions of dollars of venture capital in US start-ups, despite pushback from President Trump's administration and the European Union (*The Economist* 2018m; 2018q). Much of this activity is helped by the specific ways in which Chinese firms have adapted to the Chinese business environment, which is characterized by shaky rule of law, massive consumer scale, extremely changeable demand, cutthroat competition and proximity to an efficient low-cost manufacturing hub. Whereas US firms have developed to take advantage of their own more stable and business-friendly environment, with high breadth of ownership and relatively transparent management, Chinese firms are often closely associated with a celebrity boss/owner with majority control (unlike even Mark Zuckerberg or Steve Jobs), and display highly opportunistic behaviour, expanding quickly into new markets (thereby resembling the sprawling conglomerates of old) (*The Economist* 2018g). Kai-Fu Lee has argued that Chinese companies are hungrier, less complacent, more vigorous, more eager for competition, and less constrained by mission statements and core values than their US counterparts (Lee 2018). Furthermore, according to the same author, the age of the massive AI breakthroughs, where the United States has been a leader, is being superseded by an age of implementation, of applying and adapting the algorithms to the dull problems of everyday life. Here, China has the advantage, both in terms of the national skillset, and in terms of the numbers of scientists it can deploy (ibid.).

Another growing source of advantage for China is its trove of data, the raw material of AI (ibid.). China's internet economy generates far more data than any other, partly because of its size and partly because much Chinese commerce has moved on from cash to electronic payments. The social media app WeChat has become dominant in China, not only for communication with friends, family and work colleagues but also for mobile payments. Expatriate Chinese are increasingly using WeChat and it has started to spread throughout the West as a result. All the data is stored in China and therefore accessible to the Chinese government. Furthermore, unhindered by data protection regulation or

noticeable public demand for privacy, data is gathered from many other sources, including closed circuit television. This data is immensely important to Chinese science but also augmented by various schemes in which Chinese citizens rate each other as citizens on social networks. China hopes to lead in AI and has made advances in areas such as face recognition and autonomous vehicles. Its less-developed status helps as well, in terms of social and industrial adaptability; whereas the United States is restricting the use of self-driving cars and worrying about pedestrian deaths (*The Economist* 2018b), China is building a city to accommodate them (Lee 2018).

Beyond its borders, China's influence on American firms is growing. In 2018, it forced Apple to transfer its iCloud data about Chinese users to a Chinese data centre (*The Economist* 2018r). Of course, this kind of nationalism is common across the world, including in the European Union, but it does mean that the government can certainly get hold of this valuable data more easily. Business in the lucrative Chinese market will have to be done on Chinese terms. In 2010, Google quit China in order to avoid having to censor search results. At the time of writing, it is reported that Google is testing a mobile search app called "Dragonfly," which would filter websites blocked by China's "Great Firewall," and provide instead a notice that some results might have been removed. If it goes ahead, it would have to compete with Baidu, which carries out 75 percent of searches in China, and which has cemented its dominance by ensuring that its own apps are pre-installed on Chinese smartphones (ibid.).

In 2013, President Xi Jinping unveiled an infrastructure and trade initiative, entitled the Silk Road Economic Belt and the Twenty-first-Century Maritime Silk Road, often called "The Belt and Road Initiative." This aims to link together the Eurasian world with connectivity and cooperative ventures, as a route for future Chinese (and other) trade, by developing infrastructure across Asia, Europe and Africa. The authoritarian internet could well become part of this project, leading to a Belt, Road and Information Superhighway Initiative, comprising the technological areas where China sees potential advantage, including AI, big data, quantum computing and cloud storage. The city of Xi'an in Shaanxi province, a bastion of the original medieval Silk Road, has already positioned itself as a tech centre (*The Economist* 2018e).

Such an internet might easily be supported by poorer countries for which the internet has proved problematic — for instance, countries including Mauretania, Algeria, Uzbekistan, Iraq and Ethiopia have been forced to turn the internet off during school exam time, because of the prevalence of cheating (*The Economist* 2018h). While Chinese companies have been increasingly targeted by nationalists in the United States, and major US firms apart from Amazon and Apple are pretty well barred from China, the major Chinese and American firms compete in other markets, such as Brazil, Indonesia, India and Africa. In January 2019, the planet is on course to achieve a figure of 50 percent of its population connected to the internet, but with much of the remaining 50 percent in rural China, India and Africa. China has a considerable financial influence in Africa and will seek to influence the governance of the internet there. It may do this under the radar; while US firms tend to transplant their usual services into the new markets under their own names, tweaking where necessary, Chinese firms have a somewhat more covert strategy of buying stakes in promising start-ups (as they have even in the United States before getting pushback from the Trump administration) — 2017 saw US$5 billion invested in Indian start-ups by Chinese tech firms (*The Economist* 2018i).

DC's Commercial Internet

The characteristics of what might be called the "DC commercial internet" — the vision of the commercial internet as espoused by leaders in the US Capitol — are similar to those of the Silicon Valley open internet — and indeed, commercial and technology interests have always cooperated strongly through the internet's history, helped by their geographical concentration in the same nation. However, the United States is now polarized to an unprecedented degree, and the champions of the DC model, in particular the Republicans, notably President Trump, are at loggerheads (over a tremendous number of issues) with the champions of the Silicon Valley model, in particular the Democrats and Barack Obama, whose White House hosted a number of present and former technologists. Most prominently, the Federal Communications Commission (FCC) voted in December 2017 by three to two to repeal its commitment to net neutrality that it had brought in under the previous administration in 2015. The *Star Wars* actor Mark Hamill criticized the FCC for siding with large corporations against the

individual; Senator Ted Cruz replied that Darth Vader would have approved of regulating the internet (*The Economist* 2017c). The head of the FCC, Ajit Pai (appointed to the FCC by President Obama, but elevated to its chair by President Trump), claims to be a supporter of net neutrality but argues that federal regulation will suppress innovation, and that net neutrality ought to be a contractual matter between ISPs and their customers, in their terms and conditions (*The Economist* 2017a).

The roots of the Silicon Valley/DC split lie in the collective action problem that affects internet operators (DeNardis 2014a). These operators compete with each other for their customers, but on the other hand, their cooperation in connecting their networks with each other, using standard protocols and handling their competitors' traffic, makes the internet the internet, rather than a series of disconnected or weakly connected islands. This creates a tension between what we might think of as the public good of a seamless internet, and the private interests of these operators. The tension has led to much creation and innovation, but the line between the public and the private good can shift. Silicon Valley's open internet focuses on the public, while DC's commercial internet leverages the interests of private actors, on the argument that large profits show that public interests are indeed being served by these self-interested actors. For example, in contrast to the European Union's approach under Commissioner Vestager (see above), US trustbusters are more tolerant of the monopolistic tendencies of the industry, following an argument of Joseph Schumpeter that the promise of monopoly profits can be an important driver of innovation and customer service (Schumpeter 2010, 76–92). Having said that, even the Silicon Valley firms can be torn. Facebook, for example, is a prime builder of the walled gardens that Jonathan Zittrain (2008) railed against, while the tech giants are so keen to buy start-ups that they are threatening the start-up culture for which Silicon Valley is famous (*The Economist* 2018f; 2018t).

This dilemma is exacerbated by its being located in the United States, where the extent and limits of free speech are a matter of major constitutional interest. The First Amendment forbids the state to curb free speech, but jurisprudence has led to divergent interpretations. The affirmative interpretation, which held sway during much of the twentieth century, holds that the state is justified in intervening in public spaces for expression (even ones that are privately owned, such as telecommunications and internet spaces), to support the societal goal of facilitating expression of a multiplicity of viewpoints and, conversely, restricting the rights of the owners of these spaces to censor or limit the messages they carry. The negative interpretation is that the First Amendment forbids the state from intervening in such spaces, as to do so would restrict the free speech rights of the owners to determine what voices are heard in their spaces; this interpretation has been the majority view of the Supreme Court since the 1980s. In short, does the state have a positive duty to make sure speech is promoted, even on private property, or does the First Amendment's scope only cover publicly administered spaces, so that private property owners' rights are unaffected by it (Nunziato 2009)? The positive interpretation favours net neutrality and Silicon Valley openness, while the negative interpretation (at the time of writing in the legal ascendant) favours private property interests. It is a parochial argument to the rest of us, but the way it plays out will affect the internet as a whole.

There are engineering arguments for limited traffic discrimination, such as to manage the network and to ensure that quality of service is maintained for all — for example, during busy periods, it might be acceptable to slow down content that is not so time-critical, such as email. But most arguments against net neutrality have strong business reasons. Internet providers are the organizations that would have to obey any net neutrality law, such as the regulations brought in by the FCC in 2015 under Obama, and they are generally opposed, preferring not to have constraints on their network management. Neo-liberal free-market thinkers are also opposed, not only because they generally oppose government regulation on ideological grounds but also because they support free market solutions to problems based on freedom to exploit property rights (the providers are seen, on this view, as owners of the network, and so should be free to manage them as they see fit). If anyone is treated unfairly, then they should have recourse to a private legal challenge, rather than protection via regulation, so that regulation would happen "organically" via common law. We see here a clash between two types of liberty supported under liberalism, as described by Isaiah Berlin (2002): "freedom from" (in this case, censorship) versus "freedom to" (in

this case, manage one's private property, that is, the internet infrastructure owned by providers).

More widely, this property-based model threatens the interoperability that was a fundamental principle of the internet and, subsequently, the Web — Berners-Lee in his 2018 Turing Lecture[9] argued that the universality of identifiers for online resources was key for the added value of the Web. As early as 2008, Zittrain sounded an alarm about what he called non-generative models of the internet, which created walled gardens and undermined innovation (Zittrain 2008). Since Zittrain wrote, the extraordinary growth of social networking has built the walls around the gardens still higher, while arguably making the gardens prettier and more habitable.

In particular, social networking sites (SNSs) bypass some of the internet's interoperability mechanisms. They do not particularly support cross-platform compatibility (so that interacting between two SNSs is not as simple as, say, sending an email from Gmail to an .edu address). Personal data is not portable between sites, although the GDPR is attempting to change this. Search is restricted. Resources are not identified or located by universal formalisms (DeNardis 2014b). As Berners-Lee wrote in 2010, "connections among data exist only within a site. So the more you enter, the more you become locked in. Your [SNS] becomes…a closed silo of content…The more this kind of architecture gains widespread use, the more the Web becomes fragmented, and the less we enjoy a single, universal information space" (quoted in DeNardis 2014a, 241). Zittrain and Berners-Lee defend the Silicon Valley open internet, but the DC commercial response is that SNSs provide services that people actually wish to access, in large numbers, and that the only responsibilities SNS owners have are to their customers, assuming that they do not interfere with the running of the internet as a whole. As with other types of property, if someone wishes to build a wall around their garden, they should be allowed to do so as long as they cause no harms elsewhere. They should be the best judge of the value to be obtained from their property. The single, universal information space that Berners-Lee advocates cannot and should not be imposed, on this view, against the will of someone to monetize their intellectual property via restriction.

9 See https://amturing.acm.org/vp/berners-lee_8087960.cfm.

Addendum: Moscow's Spoiler Model

As noted above, geopolitical shifts have led to a lessening of the constraints on Russia and a reassertion of the imperial geography of the past (Kaplan 2018). Russia under President Vladimir Putin has exploited this to engineer an ideological space opposed to the West, based on a mystical mélange of nationalism and destiny, *ressentiment* and victimhood, power and calculation, cynicism and conspiracy theories (Snyder 2018). Given this vision, the decentralized internet, with no institutionalized editing or fact-checking, has been an ally. Indeed, the polarization of politics in the West, notably in the United States but also in the European Union, has provided the opportunity to import the uncertainties and obfuscations routine in Russian politics into Western politics, by cheaply importing narratives, arguments and conspiracies using the power of bots. Much of this has been revealed by Robert Mueller's inquiry into Russian interference in the 2016 US presidential election (*The Economist* 2018a).

There are several other instances of this, which appear strategically inexplicable except as a means of sowing division and mistrust. For instance, David A. Broniatowski et al. (2018) report that Russian bots and trolls regularly tweet about vaccination in divisive terms, linking the issues to controversies in American politics. The tweets are both pro- and anti-vaccination, but the purpose appears to be less to establish a position as to create, by the volume of tweets, the impression of strong and partisan debate, and to recruit partisan campaigners by associating vaccination with the several other wedge issues in America's dysfunctional politics.

This is not just a Russian tactic (although the term "disinformation" was indeed originally a Russian term, coined during the Stalin era). No doubt all nations indulge in deliberately propagating falsehood. However, disinformation is a particularly potent weapon against the West, where speech is freer (and it is easier to spread ideas), and where controlling the public sphere is seen as rather alien. A recent report from the Oxford Internet Institute argued that "computational propaganda is now one of the most powerful tools against democracy" (Woolley and Howard 2017, 7) and found evidence that, for instance, 45 percent of Twitter activity in Russia was automated for the creation of disinformation (ibid., 4), and that political debate in Germany, the United States, Poland, Brazil, Ukraine

and Taiwan is also compromised (ibid.). In August 2018, Facebook and Twitter shut down hundreds of accounts accused of spreading disinformation not only from Russia, but also from Iran (Timberg 2018).

Discussion: Four Internets and a Free Rider

These five visions of the internet do not, and probably could not, exist in their pure forms, still less be so neatly ascribed to particular regimes. They are caricatured here to make the main points: the homogeneity of the internet cannot be assumed (Global Commission on Internet Governance 2016), and scenarios about what is sometimes called its Balkanization (creating "the Splinternet") cannot be ruled out. Neither are these the only internets that could evolve — the four (plus one) could become five, or six, or seven or more. There could be a developing world internet, or a feminist internet, or an Islamic internet, or a caring internet, or an internet of cyborgs, if the appropriate ethical vision found a technological realization and sufficiently powerful institutional backing.

Many commentators have drawn the conclusion that this is a straight fight between China and the United States.[10] This notion underestimates the breadth of dispute between conflicting visions (not least within the United States itself). However, it is important to understand as well that these models do (at the moment) coexist in uneasy tension, and that (so far) all are perceived to have some value by most actors.

Russia is singled out as the spoiler, free riding on the efforts of others to produce a valuable information space. Of course, very many nations, including the United States, indulge in disinformation. The actions of the United States (under both Obama and Trump) in indicting cyber spies and cyber warriors from China, Russia, Iran and elsewhere have reportedly concerned members of its National Security Agency, who themselves fear being prosecuted outside the United States for similar crimes (*The Economist* 2018v). Meanwhile, although the Russians and others are happy to troll the internet, they do require a functioning internet to troll, so they have no incentive to undermine it totally (both the honest and the dishonest benefit from general honesty; compare Nyberg 1997; Iñiguez et al. 2014). However, the acceptability of dishonesty is likely to increase if the system as a whole is perceived as unfair, providing spoilers with incentives to highlight lapses in the standards of other nations with accusations of hypocrisy (compare, for example, Zhang 2008).

Similarly, the Chinese authoritarian model appeals to its government, which is quick to close down conversation in its lively microblogging media. However, it also values the openness that leads to the publication of dissent, which it uses as an early warning of problems with illegal land appropriations, pollution, corruption, poor food and air quality, and other issues. Conversely, the authoritarian internet will appeal to any government, however democratic, that takes responsibility for social problems (such as obesity or climate change) and would rather impose a paternalistic solution than allow one to emerge from an autonomous citizenry; the kind of soft paternalism known as the "nudge" philosophy is one means of leveraging large quantities of data within an internet environment in which choices are carefully closed down (Thaler and Sunstein 2008). India, for example, eschews the full Chinese authoritarian suite, but nevertheless has access to large quantities of social media and banking data that are highly linkable through its Aadhaar digital biometric identity scheme.

In the United States, as emphasized above, the breakdown of political consensus has made the distinction between the Silicon Valley open internet and the DC commercial internet far sharper than it traditionally has been (one of the last acts in office of President Trump's former Attorney General Jeff Sessions was to sue the State of California for its decision to restore net neutrality regulation against the FCC's own reversal [*The Guardian* 2018]), but until fairly recently the two visions managed to rub along reasonably well, with businesses switching their evangelizing between openness and property/markets opportunistically as their situations demanded. Meanwhile, some of the tech giants are recruiting prominent European politicians to explain their positions to fellow Eurocrats, such as Facebook's appointment of the former leader of Britain's Liberal Democrats, Nick Clegg, as its head

10 For example, Eric Schmidt (quoted in Kolodny 2018) and Lee, in his book *AI Superpowers: China, Silicon Valley and the New World Order* (2018).

of global affairs (Clegg 2018). Such cross-fertilization may also result in bringing the Eurocrats closer to the Americans; Margrethe Vestager's decision in 2017 to order Apple to pay back-taxes to the Irish government (that did not want the money) was criticized by one of her predecessors, Neelie Kroes, who had been appointed to Uber's Public Policy Advisory Board in 2016 (*The Economist* 2017b).

Even Tim Berners-Lee, a consistent apostle of openness, has a vision of the Web that looks much closer to Brussels' bourgeois internet than Silicon Valley's open one, in which polite conversation is not drowned out by the roughhouse — consistent with the Web's birth as a means of disseminating scientific research (Berners-Lee 2018). The initiatives he has championed — ranging from the Web We Want,[11] a project of the World Wide Web Foundation, to a "Magna Carta for the Web" (Kiss 2014; Sample 2018), to the Solid platform, which is intended to "re-decentralize" the Web guided by the principle of "personal empowerment through data"[12] — aim to promote human rights, privacy, anti-discrimination and trolling, and bear a closer resemblance to the European Commission's vision than to John Perry Barlow's. The Solid vision sees individuals curating their own data responsibly and managing read/write permissions via "PODs" — personal online data stores — thereby meeting one of Berners-Lee's own worries about the Web (that we have lost control of our personal data), but maybe not dealing with some of the by-products of openness, specifically the spread of misinformation and the lack of transparency (Berners-Lee 2017). The Global Commission on Internet Governance (2016) adopts a similar position of combining openness with a respectful environment.

Hence these models (and the spoilers that undermine them) are likely to coexist even within individual organizations and governments. Nevertheless, clear preferences exist for certain models, and these contribute to the tensions in global internet governance.

Conclusion

In 2002, when the world seemed unipolar under a benign if stern American hegemony, and the recent terrorist attacks in New York had created an imperative to reassert American moral ascendency, President George W. Bush described an "Axis of Evil." In today's very different world, we can discern a somewhat scarier "Axis of Incivility," of nation states jostling for narrow advantage, with a view of international relations, including economic relations, as zero sum. Unlike the Axis of Evil, which reflected US foreign policy concerns, the Axis of Incivility has at its foundations the three major superpowers, the United States, China and Russia, each of which in its different ways at the time of writing pursues aggressive nationalist policy goals while showing impatience with due process both internally and internationally. Many other nations, including Egypt, Hungary, India, Iran, Israel, the Philippines, Poland, Saudi Arabia and Turkey, are following this lead.

In such a world, it is inconceivable that these competing visions of the internet will not become entangled in the drive for international recognition, power and coalition-building. Neither the benefits of cooperation and openness, nor those of privacy and bourgeois stability, are likely to cut much ice with rational actors with such a mindset. Hence, the competition to establish which, if any, of the four internets will prevail (however temporarily) is likely to be strong, and not always focused on win-wins.

11 See https://webwewant.org/.

12 See https://solid.mit.edu/.

Works Cited

Bamberger, Kenneth A. and Deirdre K. Mulligan. 2015. *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. Cambridge, MA: MIT Press.

Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." Davos, Switzerland, February 8. www.eff.org/cyberspace-independence.

Benkler, Yochai. 2006. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, CT: Yale University Press.

Berlin, Isaiah. 2002. "Two concepts of liberty." In *Liberty*, edited by Henry Hardy, 166–217. Oxford, UK: Oxford University Press.

Berners-Lee, Tim. 2017. "I invented the web. Here are three things we need to change to save it." *The Guardian*, March 12. www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet.

———. 2018. "One Small Step for the Web…" Inrupt.com, September 28. www.inrupt.com/blog/one-small-step-for-the-web.

Berners-Lee, Tim, Wendy Hall, James A. Hendler, Kieron O'Hara, Nigel Shadbolt and Daniel J. Weitzner. 2006. "A Framework for Web Science." *Foundations and Trends in Web Science* 1 (1): 1–134.

Blum, Andrew. 2012. *Tubes: Behind the Scenes at the Internet*. London, UK: Viking.

Broniatowski, David A., Amelia M. Jamison, SiHua Qi, Lulwah AlKulaib, Tao Chen, Adrian Benton, Sandra C. Quinn and Mark Dredze. 2018. "Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate." *American Journal of Public Health* 108 (10): 1378–84. https://ajph.aphapublications.org/doi/10.2105/AJPH.2018.304567.

Clegg, Nick. 2018. "I'm joining Facebook to build bridges between politics and tech." *The Guardian*, October 19. www.theguardian.com/commentisfree/2018/oct/19/nick-clegg-facebook-politics-tech.

DeNardis, Laura. 2014a. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

———. 2014b. "The social media challenge to Internet governance." In *Society and the Internet: How Networks of Information and Communication Are Changing Our Lives*, edited by Mark Graham and William H. Dutton, 348–59. Oxford, UK: Oxford University Press.

EDPS Ethics Advisory Group. 2018. *Towards a Digital Ethics*. European Data Protection Supervisor. https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf.

Global Commission on Internet Governance. 2016. *One Internet*. Waterloo, ON: CIGI. www.cigionline.org/publications/one-internet.

Hunter, Philip. 2008. "Pakistan YouTube block exposes fundamental Internet security weakness: Concern that Pakistani action affected YouTube access elsewhere in world." *Computer Fraud and Security* 4: 10–11. https://doi.org/10.1016/S1361-3723(08)70065-4.

Iñiguez, Gerardo, Tzipe Govezensky, Robin Dunbar, Kimmo Kaski and Rafael A. Barrio. 2014. "Effects of deception in social networks." *Proceedings of the Royal Society B: Biological Sciences* 281 (1790). https://doi.org/10.1098/rspb.2014.1195.

Kaplan, Robert D. 2018. *The Return of Marco Polo's World: War, Strategy, and American Interests in the Twenty-First Century*. New York, NY: Random House.

Kiss, Jemima. 2014. "An online Magna Carta: Berners-Lee calls for bill of rights for web." *The Guardian*, March 12. www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web.

Kolodny, Lora. 2018. "Former Google CEO predicts the internet will split in two — and one part will be led by China." CNBC Tech, September 20. www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html.

Lee, Kai-Fu. 2018. *AI Superpowers: China, Silicon Valley and the New World Order*. New York, NY: Houghton Mifflin Harcourt.

McCloskey, Deirdre N. 2006. *The Bourgeois Virtues: Ethics for an Age of Commerce*. Chicago, IL: University of Chicago Press.

Morozov, Evgeny. 2011. *The Net Delusion: How Not to Liberate the World*. London, UK: Allen Lane.

Nunziato, Dawn C. 2009. *Virtual Freedom: Net Neutrality and Free Speech in the Internet Age*. Stanford, CA: Stanford University Press.

Nyberg, Sten. 1997. "The honest society: stability and policy considerations." *Journal of Public Economics* 64 (1): 83–99. https://doi.org/10.1016/S0047-2727(96)01608-8.

O'Hara, Kieron. 2004. *Trust: From Socrates to Spin*. Duxford, UK: Icon Books.

———. 2009. "Web engineering in the Chinese context: 'Let a hundred flowers bloom, a hundred schools of thought contend.'" In *China's Information and Communications Technology Revolution: Social changes and state responses*, edited by Xiaoling Zhang and Yongnian Zheng, 121–35. Abingdon, UK: Routledge.

———. 2015. "The Right to Be Forgotten: The Good, the Bad, and the Ugly." *IEEE Internet Computing* 19 (4): 73–79. http://doi.ieeecomputersociety.org/10.1109/MIC.2015.88.

———. 2018. "The contradictions of digital modernity." *AI and Society*, April 25. https://doi.org/10.1007/s00146-018-0843-7.

O'Hara, Kieron, Noshir S. Contractor, Wendy Hall, James A. Hendler and Nigel Shadbolt. 2013. "Web Science: understanding the emergence of macro-level features on the World Wide Web." *Foundations and Trends in Web Science* 4 (2-3): 1–165.

O'Hara, Kieron and Wendy Hall. 2013. "Web Science." In *The Oxford Handbook of Internet Studies*, edited by William H. Dutton, 48–68. Oxford, UK: Oxford University Press.

O'Hara, Kieron and Nigel Shadbolt. 2015. "The right to be forgotten: its potential role in a coherent privacy regime." *European Data Protection Law Review* 1 (3): 178–89. https://doi.org/10.21552/EDPL/2015/3/5.

O'Hara, Kieron, Nigel Shadbolt and Wendy Hall. 2016. *A Pragmatic Approach to the Right to Be Forgotten*. Global Commission on Internet Governance Paper Series No. 26. Waterloo, ON: CIGI. www.cigionline.org/publications/pragmatic-approach-right-be-forgotten.

Politou, Eugenia, Efthimios Alepis and Constantinos Patsakis. 2018. "Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions." *Journal of Cybersecurity*. http://doi.org/10.1093/cybsec/tyy001.

Prosser, William L. 1960. "Privacy." *California Law Review* 48: 383–423.

Sample, Ian. 2018. "Tim Berners-Lee launches campaign to save the web from abuse." *The Guardian*, November 4. www.theguardian.com/technology/2018/nov/05/tim-berners-lee-launches-campaign-to-save-the-web-from-abuse.

Schumpeter, Joseph. 2010. *Capitalism, Socialism and Democracy*. Abingdon, UK: Routledge Classics.

Snyder, Timothy. 2018. *The Road to Unfreedom*. London, UK: Bodley Head.

Solove, Daniel. 2014. "Privacy and Data Security Violation: What's the Harm?" *TeachPrivacy* (blog), July 2. https://teachprivacy.com/privacy-data-security-violations-whats-harm/.

Thaler, Richard H. and Cass R. Sunstein. 2008. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New Haven, CT: Yale University Press.

The Economist. 2017a. "Another debate about net neutrality in America." *The Economist*, April 22.

———. 2017b. "Is Margrethe Vestager championing consumers or her political career?" *The Economist*, September 14.

———. 2017c. "A vote on 'net neutrality' has intensified a battle over the internet's future." *The Economist*, December 23.

———. 2018a. "Russian disinformation distorts American and European democracy." *The Economist*, February 24.

———. 2018b. "A pedestrian has been killed by a self-driving car." *The Economist*, March 24.

———. 2018c. "Who will be the main loser from Europe's new data-privacy law?" *The Economist*, May 26.

———. 2018d. "China has turned Xinjiang into a police state like no other." *The Economist*, June 2.

———. 2018e. "China talks of building a 'digital Silk Road.'" *The Economist*, June 2.

———. 2018f. "American tech giants are making life tough for startups." *The Economist*, June 2.

———. 2018g. "Xiaomi's forthcoming IPO shows how the rules of business are changing." *The Economist*, June 9.

———. 2018h. "Why some countries are turning off the internet on exam days." *The Economist*, July 7.

———. 2018i. "Chinese and US tech giants go at it in emerging markets." *The Economist*, July 7.

———. 2018j. "China's new $15bn tech fund emulates SoftBank's Vision Fund." *The Economist*, July 14.

———. 2018k. "The backlash against Airbnb." *The Economist*, July 21.

———. 2018l. "WhatsApp suggests a cure for virality." *The Economist*, July 28.

———. 2018m. "America and the EU are both toughening up on foreign capital." *The Economist*, July 28.

———. 2018n. "Why Swedes are inserting microchips into their bodies." *The Economist*, August 4.

———. 2018o. "Britain's spies get entrepreneurial." *The Economist*, August 4.

———. 2018p. "Alibaba and Tencent have become China's most formidable investors." *The Economist*, August 4.

———. 2018q. "Silicon Valley gets queasy about Chinese money." *The Economist*, August 11.

———. 2018r. "Plans for a return to China has many up in arms." *The Economist*, August 25.

———. 2018s. "Why startups are leaving Silicon Valley." *The Economist*, September 1.

———. 2018t. "Silicon Valley is changing, and its lead over other tech hubs narrowing." *The Economist*, September 1.

———. 2018u. "A controversial new copyright law moves a step closer to approval." *The Economist*, September 15.

———. 2018v. "America's government is putting foreign cyber-spies in the dock." *The Economist*, September 15.

The Guardian. 2018. "US justice department sues California over new net neutrality law." *The Guardian*, October 1. www.theguardian.com/technology/2018/oct/01/us-justice-department-sues-california-to-over-new-net-neutrality-law.

Timberg, Craig. 2018. "Facebook, Twitter remove hundreds of disinformation pages created by Russia, Iran." *The Sydney Morning Herald*, August 22. www.smh.com.au/world/north-america/facebook-removes-652-disinformation-pages-created-by-russia-iran-20180822-p4zyyi.html.

Whitman, James Q. 2004. "The two Western cultures of privacy: dignity versus liberty." *Yale Law Journal* 113: 1151–221.

Woolley, Samuel C. and Philip N. Howard. 2017. *Computational Propaganda Worldwide: Executive Summary*. Working Paper 2017.11. Oxford, UK: Oxford Internet Institute. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

Working Group on Internet Governance. 2005. *Report from the Working Group on Internet Governance*. Document WSIS-II/PC-3/DOC/5-E, August 3. www.itu.int/net/wsis/docs2/pc3/off5.pdf.

Zhang, Yue. 2008. "The effects of perceived fairness and communication on honesty and collusion in a multi-agent setting." *Accounting Review* 83 (4): 1125–46. https://doi.org/10.2308/accr.2008.83.4.1125.

Zittrain, Jonathan. 2008. *The Future of the Internet: And How to Stop It*. New Haven, CT: Yale University Press.

About CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

À propos du CIGI

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan doté d'un point de vue objectif et unique de portée mondiale. Nos recherches, nos avis et nos interventions publiques ont des effets réels sur le monde d'aujourd'hui car ils apportent de la clarté et une réflexion novatrice pour l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques mondiales, et le droit international, et nous les exécutons avec la collaboration de nombreux partenaires stratégiques et le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline